QUESTION 1293
A penetration tester has successfully accessed a web server using an exploit in the user-agent string for Apache Struts. The tester then brute forces a credential that provides access to the back-end database server in a different subnet. This is an example of:

A. persistence
B. pivoting
C. escalation of privilege
D. a remote access Trojan

Answer: B

QUESTION 1294
A software development company needs to augment staff by hiring consultants for a high-stakes project. The project has the following requirements:
- Consultants will have access to highly confidential, proprietary data.
- Consultants will not be provided with company-owned assets.
- Work needs to start immediately.
- Consultants will be provided with internal email addresses for communications.
Which of the following solutions is the BEST method for controlling data exfiltration during this project?

A. Require that all consultant activity be restricted to a secure VDI environment
B. Require the consultants to sign an agreement stating they will only use the company-provided email address for communications during the project
C. Require updated antivirus, USB blocking, and a host-based firewall on all consultant devices
D. Require the consultants to connect to the company VPN when accessing confidential resources

Answer: A

QUESTION 1295
In which of the following ways does phishing and smishing differ?

A. One is primarily based on social engineering, and the other is based on evading spam filters
B. One uses SMS as a delivery mechanism, and the other uses email
C. Smishing relies on hard-wired connections and mobile code updates
D. Phishing leverages poor email tagging to exploit SPIM settings

Answer: B

QUESTION 1296
A security analyst is determining the point of compromise after a company was hacked. The analyst checks the server logs and sees that a user account was logged in at night, and several large compressed files were exfiltrated. The analyst then discovers the user last logged in four years ago and was terminated. Which of the following should the security analyst recommend to prevent this type of attack in the future? (Choose two.)

A. Review and update the firewall settings
B. Restrict the compromised user account
C. Disable all user accounts that are not logged in to for 180 days
D. Enable a login banner prohibiting unauthorized use
E. Perform an audit of all company user accounts
F. Create a honeypot to catch the hacker

Answer: BE

QUESTION 1297
An analysis of a threat actor, which has been active for several years, reveals the threat actor has high levels of funding, motivation, and sophistication. Which of the following types of threat actors does this BEST describe?

A. Advanced persistent threat
B. Hacktivist
C. Organized crime
D. Insider

Answer: A

QUESTION 1298
Given the following output:

```
NMAP -P 80 ==script hostmap=bfk.nse company.com
starting NMAP 6.46
NMAP scan report for company.com (172.255.240.169)

Port State Service
80/TCP open http

Host script results
hostmap-bfk
hosts:
172.255.240.169
web1.company.com
swebdb1.company.com
web3.company.com
swebdb2.company.com

NMAP done: scanned in 2.10 seconds
```

Which of the following BEST describes the scanned environment?

A. A host was identified as a web server that is hosting multiple domains
B. A host was scanned, and web-based vulnerabilities were found
C. A connection was established to a domain, and several redirect connections were identified
D. A web shell was planted in company.com's content management system

Answer: B

QUESTION 1299
When an initialization vector is added to each encryption cycle, it is using the:

A. ECB cipher mode
B. MD5 cipher mode
C. XOR cipher mode
D. CBC cipher mode

Answer: D

QUESTION 1300
During a routine check, a security analyst discovered the script responsible for the backup of the corporate file server has been changed to the following:

```
date = get_currentdate()
if date = $userA.Birthdate then
   exec ' rm -rf /'
end if
```

Which of the following BEST describes the type of malware the analyst discovered?

A. Keylogger
B. Rootkit
C. RAT
D. Logic bomb

Answer: D

QUESTION 1301
An organization requires three separate factors for authentication to sensitive systems. Which of the following would BEST satisfy the requirement?

A. Fingerprint, PIN, and mother's maiden name
B. One-time password sent to a smartphone, thumbprint, and home street address
C. Fingerprint, voice recognition, and password
D. Password, one-time password sent to a smartphone, and text message sent to a smartphone

Answer: B

QUESTION 1302
A security analyst has been asked to implement secure protocols to prevent cleartext credentials from being transmitted over the internal network. Which of the following protocols is the security analyst MOST likely to implement? (Choose two.)

A. SNMPv3
B. S/MIME
C. DNSSEC
D. SSH
E. SFTP

Answer: DE

QUESTION 1303
Buffer overflow can be avoided using proper:

A. memory leak prevention
B. memory reuse
C. input validation
D. implementation of ASLR

Answer: C

QUESTION 1304
Which of the following systems, if compromised, may cause great danger to the integrity of water supplies and their chemical levels?

A. UAV
B. SCADA
C. HVAC
D. MFD

Answer: B

QUESTION 1305
An organization has the following written policies:
- Users must request approval for non-standard software installation.
- Administrators will perform all software installations.
- Software must be installed from a trusted repository.
A recent security audit identified crypto-currency software installed on one user's machine. There are no indications of compromise on this machine. Which of the following is the MOST likely cause of this policy violation and the BEST remediation to prevent a reoccurrence?

A. The user's machine was infected with malware; implement the organization's incident response
B. The user installed the software on the machine; implement technical controls to enforce the written policies
C. The crypto-currency software was misidentified and is authorized; add the software to the organization's approved list
D. Administrators downloaded the software from an untrusted repository; add a policy that requires integrity checking for all software.

Answer: B

QUESTION 1306
Penetration testing is distinct from vulnerability scanning primarily because penetration testing:

A. leverages credentialed scanning to obtain persistence
B. involves multiple active exploitation techniques
C. relies exclusively on passive exploitation attempts for pivoting
D. relies on misconfiguration of security controls

Answer: B

QUESTION 1307
Employees receive a benefits enrollment email from the company's human resources department at the beginning of each year. Several users have reported receiving the email but are unable to log in to the website with their usernames and passwords. Users who enter the URL for the human resources website can log in without issue. Which of the following security issues is occurring?

A. Several users' computers were not configured to use HTTPS to access the website

B. The human resources servers received a large number of requests, resulting in a DoS
C. The internal DNS server was compromised, directing users to a hacker's server
D. Users received a social engineering email and were directed to an external website

Answer: D

QUESTION 1308
An engineer is configuring a wireless network using PEAP for the authentication protocol. Which of the following is required?

A. 802.11n support on the WAP
B. X.509 certificate on the server
C. CCMP support on the network switch
D. TLS 1.0 support on the client

Answer: B

QUESTION 1309
An organization is setting up a satellite office and wishes to extend the corporate network to the new site.
Which of the following is the BEST solution to allow the users to access corporate resources while focusing on usability and security?

A. Federated services
B. Single sign-on
C. Site-to-site VPN
D. SSL accelerators

Answer: C

QUESTION 1310
A NIPS administrator needs to install a new signature to observe the behavior of a worm that may be spreading over SMB. Which of the following signatures should be installed on the NIPS?

A. PERMIT from ANY:ANY to ANY:445 regex `.*SMB.*'
B. DROP from ANY:445 to ANY:445 regex `.*SMB.*'
C. DENY from ANY:ANY to ANY:445 regex `.*SMB.*'
D. RESET from ANY:ANY to ANY:445 regex `.*SMB.*'

Answer: C

QUESTION 1311
An organization uses an antivirus scanner from Company A on its firewall, an email system antivirus scanner from Company B, and an endpoint antivirus scanner from Company C. This is an example of:

A. unified threat management
B. an OVAL system
C. vendor diversity
D. alternate processing sites

Answer: C

QUESTION 1312
Exploitation of a system using widely known credentials and network addresses that results in DoS is an example of:

A. improper error handling

B. default configurations
C. untrained users
D. lack of vendor support

Answer: B

QUESTION 1313
Which of the following is an example of the second A in the AAA model?

A. The encryption protocol successfully completes the handshake and establishes a connection
B. The one-time password is keyed in, and the login system grants access
C. The event log records a successful login with a type code that indicates an interactive login
D. A domain controller confirms membership in the appropriate group

Answer: D

QUESTION 1314
Which of the following threat actors is motivated primarily by a desire for personal recognition and a sense of accomplishment?

A. A script kiddie
B. A hacktivist
C. An insider threat
D. An industrial saboteur

Answer: A